REPORT DOCUMENTATION PAGE	Form Approved OMB NO. 0704-0188

The public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggesstions for reducing this burden, to Washington Headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington VA, 22202-4302. Respondents should be aware that notwithstanding any other provision of law, no person shall be subject to any oenalty for failing to comply with a collection of information if it does not display a currently valid OMB control number.
PLEASE DO NOT RETURN YOUR FORM TO THE ABOVE ADDRESS.

1. REPORT DATE (DD-MM-YYYY) 03-06-2009	2. REPORT TYPE Final Report	3. DATES COVERED (From - To) 1-Jun-2006 - 31-May-2009

4. TITLE AND SUBTITLE Robust and Secure Localization	5a. CONTRACT NUMBER W911NF-06-1-0204
	5b. GRANT NUMBER
	5c. PROGRAM ELEMENT NUMBER 611102
6. AUTHORS John A. Stankovic	5d. PROJECT NUMBER
	5e. TASK NUMBER
	5f. WORK UNIT NUMBER

7. PERFORMING ORGANIZATION NAMES AND ADDRESSES University of Virginia Office of Sponsored Programs 1001 N. Emmett St. P.O. Box 400195 Charlottesville, VA 22904 -4195	8. PERFORMING ORGANIZATION REPORT NUMBER
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES) U.S. Army Research Office P.O. Box 12211 Research Triangle Park, NC 27709-2211	10. SPONSOR/MONITOR'S ACRONYM(S) ARO 11. SPONSOR/MONITOR'S REPORT NUMBER(S) 49545-CS.1

12. DISTRIBUTION AVAILIBILITY STATEMENT
Approved for public release; distribution unlimited

13. SUPPLEMENTARY NOTES
The views, opinions and/or findings contained in this report are those of the author(s) and should not contrued as an official Department of the Army position, policy or decision, unless so designated by other documentation.

14. ABSTRACT

The goals of this contract were to develop new solutions for robustness and security in wireless sensor networks with particular attention to localization. Our results are broad and fall into multiple areas. We developed new solutions for robust localization (section 2), secure localization (section 3), self-healing (section 4), anti-jamming (section 5) and robust wireless sensor network communication via coding (section 6). This report also includes a list of publications produced, general activities, names of graduate students supported, and several miscellaneous

15. SUBJECT TERMS
sensor, sensor networks, localization, security, robustness

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	15. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON John Stankovic
a. REPORT U	b. ABSTRACT U	c. THIS PAGE U	SAR		19b. TELEPHONE NUMBER 434-982-2275

ARO
Final Report
June 2009

John A. Stankovic

1.0 Introduction

The goals of this contract were to develop new solutions for robustness and security in wireless sensor networks with particular attention to localization. Our results are broad and fall into multiple areas. We developed new solutions for robust localization (section 2), secure localization (section 3), self-healing (section 4), anti-jamming (section 5) and robust wireless sensor network communication via coding (section 6). This report also includes a list of publications produced, general activities, names of graduate students supported, and several miscellaneous items.

2.0 Robust Localization

Despite the research efforts made by a large community, no localization system has emerged as a robust, practical, solution for the node localization problem in realistic, complex, outdoor environments. In our work, we argue that the existing localization algorithms, individually, work well for single sets of assumptions. These assumptions do not always hold, as in the case of outdoor, complex environments. In our work we showed that complex, more robust, localization systems can be built by composing localization schemes that each has limitations. See [5].

Our current localization framework is just a small part of the more complete solution that will allow a non-expert to build a robust and efficient localization system for a particular WSN deployment. Several areas require further research: development of higher level abstractions for composing localization protocols (we aim to provide a programming tool, with a script-like language, for building a localization system from individual localization protocols); development of an analysis tool that evaluates the correctness of a hierarchical localization framework and, possibly, gives soft-guarantees (e.g., largest expected localization error and the overhead required to achieve it); optimization of simultaneous executions of protocols that use, for example, radio communication (instead of having each protocol send/receive its own messages, an aggregation of data contained in these messages may significantly reduce the communication overhead); analysis of robustness against malicious attacks (due to localization protocol multi-modality, it is more difficult for an attacker to compromise the integrity of the node localization service). To date we have developed a composition based solution, identified these new problems to be addressed, and published the work in the *Networks* Journal. See [7].

3.0 Secure Localization

We have designed preliminary solutions for secure walking GPS and secure Spotlight. These, along with several secure localization schemes from the literature, will serve as components in our localization hierarchy. We will further analyze these solutions, and then implement and evaluate them. Integrating localization and secure localization protocols into a compositional hierarchy still has very interesting open questions. We now provide a few more details on secure walking GPS and secure Spotlight. Results in these areas are still preliminary.

3.1 *Secure walking GPS*: Walking GPS is a practical solution for localization in manually deployed scenarios. In this solution, a GPS Mote obtains the current global location information from a GPS device using a serial port, translates it into local location information by referencing a known Reference Point, and then passes this local copy to the currently deployed sensor node through a wireless link. While the current Walking GPS solution works well in friendly environment and is designed to deal with a number of real concerns, this solution is not secure. An attacker within radio range may deliberately perform one or more of the following to compromise localization:

- spoof GPS signals, so that the GPS device gets a false location.
- send jamming messages to disrupt normal communication between the GPS Mote and a sensor node. This makes a node unable to be localized within a given period of time.
- inject fake location information to a sensor node before the legitimate message from the GPS Mote is sent. This binds an attacker-chosen location to the nodes as they are deployed.
- establish wormhole links and tunnel legitimate messages to distant locations in the network which are beyond the radio range of the source nodes. The wormhole attack can potentially introduce significant localization error of any node which needs to be localized using the location information of its neighboring nodes in Phase 2, because this attack can easily deceive the unlocalized node into believing that a distant node is one of its neighboring nodes.

As a first step in our research we are making this non-secure design secure by solving the following problems assuming that attacks are occurring while we are localizing the nodes. A complete solution would include:

- Use military GPS with a sophisticated coding scheme to make it hard for the attacker to spoof GPS signals.
- Install a custom application (e.g., toggling a led) onto the sensor nodes to indicate a timeout of localization. This can be used to detect temporary jamming by an attacker. These un-localized nodes shall be localized later when jamming is not present.

- Authenticate and/or encrypt communication between the GPS Mote and the sensor nodes by employing a link layer (e.g., TinySec) or end-to-end encryption mechanism (e.g., AMSecure - hardware AES). This is facilitated by the need to communicate securely only between the GPS Mote and each of the sensor nodes. Since the main cost of Walking GPS is amortized to the GPS Mote, it is feasible to consider that all pair-wise keys will be stored on this GPS Mote. Alternatively, the GPS Mote can communicate (in a wired manner) with a storage device that has, for practical purposes, unlimited storage.
- Develop a collaboration-based (consensus/voting) localization algorithm at the final deployment stage to help localize the unlocalized nodes as well as correct the unrealistic location results.

Currently, this work is being evaluated and once complete will be submitted for publication.

3.2 *Secure Spotlight:* Spotlight, similar to Walking GPS, also employs an asymmetric architecture in which sensor nodes do not possess any additional hardware than what they currently have. All the sophisticated hardware and computation reside on an event-generating device. In the Spotlight localization scheme, a single device generates controlled light events aerially over predefined traces. The field sensors detect the light events and report to the base station the time at which they detected such events. Then the base station computes the locations of these sensor nodes using the spatio-temporal properties of the generated events.

Despite the good properties like low cost and high accuracy, the Spotlight localization scheme is not secure. The vulnerabilities of Spotlight lie in the existence of a “sensing channel” between the field nodes and the event-controlling device, exclusively through which communication for node localization is done. Therefore, a secure solution needs to consider attacks against this channel and involve countermeasures to deal with these attacks. Possible attacks have been listed below.

- The sensed report from field sensors to the base station may be disrupted or tampered on the way by an attacker. This will result in arbitrarily large localization errors.

- Time synchronization protocol may be compromised, inducing clock inaccuracies that disrupt the event to location mappings.

- An attacker may also generate specific light events to mislead the field sensor nodes. Therefore, field sensor nodes must be able to detect such an attack.

The research directions to be pursued are:

- Use a combination of authentication and encryption for the messages sent between the sensor nodes and the base station.
- Develop a system that does not depend on time synchronization protocol that is propagated hop by hop, through the radio channel, and instead use the sensing channel for synchronizing nodes from time to time.
- Remove the need for sending detected events from sensor nodes to the base station for location computation. Instead, pre-populate all events within sensor nodes before deployment. Then, these nodes will be able to find their own locations immediately after all events have occurred.
- Explore more complex event distribution functions that are hard for an attacker to forge. For example, we may add synchronizing header events before the light events. Or we may use pseudorandom codes to encode light event patterns. However, this may pose a great demand for more delicate sensing hardware.
- The temperature change due to laser radiation hitting the field sensor nodes is supposed to follow some propagation model (which is a function of the altitude of the aerial laser-generating device, its power, and the beam). Therefore, we may utilize thermistors on the sensor nodes to validate the identity of the incoming light event.

4.0 Self-Healing

Wireless sensor networks are now being widely used for mission critical applications such as infrastructure monitoring, fire fighting, pollution control, assisted living, military surveillance and tracking. These systems will often need to exist for years, and operate reliably in the context of real world communication, sensing and failure realities. However, due to the negative impact of noisy environments and the unreliable nature of the cheap sensor nodes being used, it has been commonly observed and reported that wireless sensor network systems are subject to performance degradations, component faults, and even major system failures in real world deployments. Our key observation is that a wireless sensor network system may drift to disorder and lose its key capabilities over time due to faults, performance degradations, node failures, security attacks, workload changes, and natural deterioration such as reduced energy and clock drift, unless proper self-healing services can be applied to maintain order, or to recover the system from disorder.

In modern large scale complex wireless sensor network systems, it is common practice to have multiple protocols and dozens of components integrated to perform a single application. The inherent complexity of these systems makes self-healing a difficult problem. Self-healing services can’t be trivially composed and provided, due to the intricate coupling and complex dependency relationships among different parts of the system. Rather dependency relationships among different components must be carefully studied, explicitly articulated and respected when designing the self-healing services. What’s even worse, the system may evolve over time, and components may be added, deleted, and updated, each change potentially impacting the dependency relationships and thus invalidate the previous design of the self-healing solution. In addition to challenges in system design and maintenance, severe resource constraints of the sensor nodes put the efficiency of the self-healing services as important. Thus, self-healing services must be efficient in terms of energy cost, message overhead and code footprints.

In our work [8][12], we developed a novel dependency constraint directed self-healing framework, to allow users to compose self-healing services both systematically and consistently, and to be able to perform self-healing services in an energy efficient manner. The framework also permits flexibility in more easily modifying the self-healing services over time rather than re-implementing the system. The major contributions of our work are: 1) a novel dependency constraint directed self-healing framework to allow users to easily compose self-healing services for large complex wireless sensor networks in systematic and consistent ways; 2) articulating 4 types of WSN dependencies; 3) by carefully identifying and adhering to the dependency constraints among different components of the system, we achieve improved efficiency in energy consumption to perform self-healing services; 4) by respecting dependency constraints in self-healing services design, we can focus on healing the components that are subject to failures only, thus we are able to keep impact on other components in the system to the minimum.

5.0 Anti-Jamming

Given limited resources for memory, computation, and energy, it is a challenge to secure wireless sensor network (WSN) nodes, particularly from denial of service attacks like jamming. Nevertheless, these attacks have been shown to be easy to perpetrate using nothing more than off-the-shelf WSN hardware to attack the network.

Security-sensitive applications, such as battlefield monitoring or surveillance, may justify the use of more resourceful devices to counter these threats. Military systems have relied on spread-spectrum communication among custom-designed, hardened devices, but even here the rapid pace of technology assimilation has created pressure to integrate commodity hardware.

Despite the availability of spread-spectrum communication on current generation WSN hardware (particularly those using the popular TI CC2420 radio transceiver), systems are still vulnerable. Spread-spectrum decreases the impact of narrowband interference from benign sources, but does not thwart an attacker unless the spreading codes or hopping sequences are unknown.

We developed the design of DeeJAM [4][10] a multi-channel medium access control (MAC) layer protocol specifically designed to satisfy the constraints of WSNs while providing resistance to jamming. It is particularly well-suited for networks that must use commodity hardware due to commercial, regulatory, or budgetary constraints. DeeJAM wraps the underlying spread-spectrum capabilities of the hardware to provide a secure, random-access MAC that raises the (currently low) threshold for the effort and resources required to successfully perpetrate jamming against WSNs.

An important property of our design is that compromised nodes are in no better position than outsiders with respect to gaining an additional advantage in jamming their neighbors' direct links (selective link jamming). Also, efficiency is critical in resource-constrained systems and figures prominently in our design.

We fully implemented and evaluated DeeJAM on an embedded platform, the MICAz mote, to obtain the most realistic and accurate results possible. In a multi-hop test with four jammers in the local neighborhood transmitting full-duty at five times the power of network nodes, DeeJAM achieved a packet delivery ratio of 92%. That is a low return for a coordinated high-power attack, and demonstrates the robustness of our solution.

The main contributions of this work are:

- A novel jamming-resistant MAC protocol with solutions to challenges in key management, synchronization, channel access scheduling, and broadcast and idle-time support. Results show high throughput and low jitter for hopping dwell times of greater than 2.2 ms.

- Security against jamming by compromised network devices through novel key and channel access management in a fully distributed coordination protocol. DeeJAM is the first MAC protocol for WSNs of which we are aware to be secure against selective link jamming.

- Efficiency in memory and execution of the protocol, especially in its generation and use of secure, pseudo-random sequences that meet embedded platform constraints and enable compromise tolerance.

- Results from an embedded implementation of DeeJAM on the MICAz platform, and empirical evaluation of its resistance to jamming attacks. With four pulse-jammers at nominal power in a single-neighborhood, packet delivery ratio is degraded by only 3% when combined with rateless erasure coding.

6.0 Reliable Communication via Codes

Often wireless sensor networks (WSNs) must reliably transfer large amounts of data, which is challenging given the typical resource constraints of WSN devices. They may be deployed in adverse circumstances where poor and highly variable link quality is caused by dynamic environmental factors such as heat and humidity, by low-cost hardware and its concomitant failure or unreliability, or by obstacles and RF interference (accidental or malicious). Whether for extracting sensor data or loading new code in over-the-air reprogramming, bulk data must be transmitted efficiently to reduce wasted computation and communication. These twin problems of loss-tolerance and efficiency are not sufficiently addressed by the state of the art.

Existing protocols use various methods to conceal or overcome loss of data blocks. The approaches taken by Deluge, RCRT, and Flush are based on Automatic Repeat Request (ARQ), in which ACKs or NACKs explicitly request retransmission of lost data. However, in severe conditions ARQ protocols require many retransmissions and have high latency for TCP in lossy networks.

Another pragmatic approach to achieving reliability in this setting is to bound the expected error rate E and use forward error correction (FEC) for transmitting blocks of the data. For predictable channel conditions, a code may be chosen that is a trade-off between overhead and performance, and it has been proven that codes exist with rate equal to the channel capacity 1-E. However, under intermittent interference or other lossy conditions, the channel may be arbitrarily bad, and for any error rate greater than E, a fixed-rate code fails completely and the block or message is lost. Pessimistically chosen parameters suffer from high overhead which must always be paid.

These limitations motivate the use of rateless erasure codes, also called fountain codes. They have recently attracted attention for use in WSNs due primarily to these properties: first, a limitless number of encoded symbols can be generated from an input of k symbols, and second, the original k symbols can be recovered from any $k' = (1 + \varepsilon)k$ received encodings (asymptotically, for fixed ε). Theoretically, no feedback channel is needed, such as for the ACKs and NACKs of an ARQ protocol. The sender can transmit an endless stream of encoded symbols and even for an arbitrarily poor channel (as long as $E < 1$), the receiver eventually receives k' symbols and can decode the message. Such an encoding scheme is optimal if $k' = k$.

We propose the use of online codes, which improve on LT codes to achieve O(1) time encoding (per block) and O(n) decoding, and which permit iterative decoding as packets are received. However, coding parameters recommended for Internet networks perform poorly in messaging overhead and memory consumption in the typical WSN operating region of relatively few data blocks. This prevents their direct replacement in existing protocols.

Our work [9] uses online codes to provide reliable data transfer despite highly lossy communication channels. To do so, it addresses challenges in the selection of appropriate parameters for the coding scheme and requires a protocol design that minimizes round-trip interactions. Our contributions include:

- We design Reliable Transfer with Online-Coding (RTOC), a novel transport protocol for WSNs that is the first to employ online codes for higher decoding efficiency than SYNAPSE. It stays synchronized despite high loss rates, and uses feedback control to adaptively terminate data transmission without ARQ as in Deluge or manual FEC selection used by Rateless Deluge.

- Through analysis of the online coding degree distribution and algorithm, we optimize parameters to trade asymptotic optimality for predictability within the WSN operating region. We achieve a 12% better effective coding rate with 72%

lower variance, which reduces the 98th percentile decoding memory requirements by 69%.

- We evaluate the performance of RTOC on an implementation in TinyOS for the MicaZ platform, and show that block delivery ratios exceed 95% despite up to 84% packet loss. Overhead follows from the page fragmentation and effective coding rate, and is low when channel loss is low.

7.0 Publications

1. A. Wood and J. Stankovic, AMSecure: Secure Link-Layer Communication in TinyOS for IEEE 802.15.4-based Wireless Sensor Networks, *ACM SenSys*, poster session, November 2006.

2. A. Wood, L. Fang, J. Stankovic, and T. He, SIGF: A Family of Configurable, Secure Routing Protocols for Wireless Sensor Networks, *ACM Security of Ad Hoc and Sensor Networks*, **Best Paper Award**, October 31, 2006.

3. H. Liu, L. Selavo, J. Stankovic, SeeDTV: Deployment Time Validation for Wireless Sensor Networks, *EMNETS*, June 2007.

4. A. Wood, J. Stankovic, and G. Zhou, DEEJAM: Defeating Energy Efficient Jamming in IEEE 802.15.4-based Wireless Networks, *IEEE SECON*, acceptance rate 20%, June 2007.

5. R. Stoleru, J. Stankovic, S. Son, Robust Node Localization for Wireless Sensor Networks, *EMNETS*, June 2007.

6. J. Stankovic, When Sensor and Actuator Networks Cover the World, invited Keynote Article, Special Issue on Ubiquitous Sensor Networks, **ETRI Journal**, Korea, Vol. 30, No. 5, Oct 2008, pp. 627-633.

7. R. Stoleru, J. Stankovic and S. Son, On Composability of Localization Protocols for Wireless Sensor Networks, special issue of **IEEE Networks**, July/August 2008.

8. Q. Cao and J. Stankovic, An In-Field Maintenance Framework for Wireless Sensor Networks, *IEEE DCOSS*, June 2008.

9. A. Wood and J. Stankovic, Online Coding for Reliable Data Transfer in Lossy Wireless Sensor Networks, *IEEE DCOSS*, June 2009.

10. A. Wood and J. Stankovic, Jamming Resistant Random-Access MAC for Wireless Sensor Networks, submitted to *CCS '09*, April 2009.

11. M. Qi, A. Wood, and J. Stankovic, Secure Walking GPS, in progress.

12. J. Li, Y. Wu, J. Stankovic, S. Son, Dependency Constraint Directed Self-Healing for Wireless Sensor Networks, in preparation.

8.0 Activities

Professor Stankovic has been active in developing a vision and a call for national research programs in cyber physical systems (includes security problems). He has also taught a graduate course on Cyber Physical Systems in Spring 2008 where concepts of realities of wireless communications and security were paramount. Other main activities include the following presentations:

- GaTech Summer School on Cyber Physical Systems, Invited Speaker, June 2009.
- Distinguished Speaker Series, Academia Sinica, Taiwan, Jan. 2010.
- Keynote Speaker, PETRA 2009, Corfu, Greece, June 2009.
- Invited Speaker, Yale University, May 8, 2009.
- Invited Panel Moderator, IPSN, April 2009.
- Invited Panel Speaker, CPS Applications, CPS Forum, SF, April 2009.
- Keynote Speaker, Aspect-Oriented Software Development Conference, March 4, 2009.
- Keynote Speaker, European Conference on Wireless Sensor Networks (EWSN 2009), Cork, Ireland, Feb. 2009.
- Invited Panelist, NSF Information Day, Cyber Physical Systems, Dec. 15, 2008.
- Invited Panelist, ICCCN, St. Thomas, August 4, 2008.
- Panel Speaker, NSF CCC meeting, Washington DC, July 7, 2008.
- Paper presentation, DCOSS, Santorini, June 13, 2008.
- Presentation, Int. Workshop on Wireless Sensor Network Research, Charlottesville, June 4, 2008.
- National Institute of Aerospace, presentation, May 12, 2008.
- Distinguished Lecture Series, University-wide, UMASS, April 30, 2008.
- Speaker, ARO PI meeting, Jan. 24, 2008.
- Keynote Speaker on CPS, RTSS '07, Arizona, Dec.6, 2007.
- Invited Speaker, Dean's Seminar in Translational Research, Univ. of Virginia Medical School, Oct. 23, 2007.
- Speaker, ULSSIS Planning meeting, Washington, DC, Oct. 18, 2007.
- Invited Panelist, NSF CDI Symposium, Albany, Sept. 6, 2007.
- Invited Speaker, National Institute for Aerospace, July 26, 2007.
- Invited Speaker, Microsoft Faculty Summit, July 16, 2007.
- Emnets, paper presentation, Cork, Ireland, June 26, 2007.
- Invited Seminar, Scuola Superiore Santa Anna, Pisa, Italy, June 20, 2007
- Keynote Speaker, HSCC 07, Pisa, Italy, April 3, 2007.
- Plenary Speaker, Symposium of the Medical Application of Ubiquitous Networks, Tokyo, Japan, March 9, 2007.
- Invited Speaker, Tokyo Medical and Dental University, March 8, 2007.

- Invited Speaker, ARO Workshop on Security in Sensor Networks, North Carolina State, Feb. 22, 2007.
- Infocom 2007, Invited Panel Participant, Alaska, May 2007.
- Distinguished Lecture Series, Iowa State, Feb. 8, 2007.
- Distinguished Lecture Series, Rutgers, Feb 28, 2007.
- Invited Speaker, Darpa ISAT meeting, Washington, D.C., Jan. 26, 2007.
- Invited Speaker, Workshop on Mathematical Challenges and Opportunities in Sensor Networking, Institute for Pure and Applied Math, UCLA, Jan. 8-12, 2007.
- Invited Panelist, SASN 2006, Washington, DC, Oct. 30, 2006.
- Keynote Speaker, Int. Conf. on Knowledge Discovery and Data Mining, Philadelphia, August 20, 2006.
- Invited Speaker (2 talks), University of Washington and Microsoft Summer Institute, August 7-9, 2006.
- Invited Speaker, NSF Planning Meeting on Cyber Physical Systems, July 27, 2006.
- Invited Speaker, HCSS Planning Meeting Workshop, NITRD, Washington, D.C., July 10, 2006.
- Keynote Speaker, Third International Conference on Networked Sensing Systems, INSS 2006, Chicago, Illinois, June 1 2006.
- Panel, EMNETS, Boston/MIT, May 30, 2006.
- Invited Speaker, Security in Sensor Networks Workshop, CMU, May 8, 2006.

9.0 Graduate Students Supported

Radu Stoleru: Completed PhD (now an Assistant Professor at Texas A and M)
Anthony Wood: Completed PhD (now a Post Doc at Univ. of Virginia)
Qiuhua Cao: PhD in progress (near completion)
Qi Mi: new PhD student

10.0 Miscellaneous

We were contacted by Mr. Frank Geck, PM, FCS IA, and Boeing Corporation both with strong interest in DeeJAM.

We were contacted by many students interested in SIGF (a secure routing protocol), which is work done in previous years. We were also contacted by UtopiaCompression with strong interest in SIGF and we wrote several SBIR proposals with them on secure routing (the latter one is still pending).

We were contacted by a company in the UK regarding interest in the localization hierarchy.